Manual de Segurança do Pix

Versão 3.6

Brasília, 19 de janeiro de 2024

SUMÁRIO

Histórico de revisão

Data	Versão	Descrição das alterações
16/01/2020	1.0	Versão inicial.
24/03/2020	2.0	• Alteração do nome do Ecossistema de Pagamentos Instantâneos para PIX; • Atualização e inclusão de referências; • Alteração da seção 1.2 e subseções para incluir o processo de assinatura digital no DICT; • Detalhamento dos processos de ativação e desativação de certificados digitais do BC e dos participantes (seções 1.3.2 a 1.3.4) • Inclusão da seção 1.3.5: Verificação da revogação de certificados digitais; • Inclusão da seção 1.4: Segurança de *QR Codes* dinâmicos.

12/08/2020	3.0	• Renumeração e reordenação das seções do Manual;
		• Inclusão da seção 6: “Logs de auditoria”;
		• Aprimoramento da seção 4: “Segurança de *QR Codes* dinâmicos”;
		• Alterações na seção 5: “Certificados digitais”, incluindo:
		  ○ Detalhamento de cada tipo de certificado digital utilizado no Pix;
		  ○ Maior clareza das regras para envio de certificados;
		  ○ Aprimoramentos nas seções de ativação, desativação e verificação de revogação de certificados.
		• Alteração no exemplo de mensagem *pacs.008* na seção 3.2;
		• Atualização de referências;
		• Correção de pequenos erros no documento.

06/10/2020	3.1	• Aprimoramentos na seção 5: “Certificados digitais”, em especial no que tange aos certificados para sites/domínios de *QR Codes* dinâmicos; • Pequenas alterações e correções no documento.
04/02/2021	3.2	• Aprimoramentos nas seções 4.2 (“Definições do padrão JWS”) e 4.3 (“Validações a serem feitas pelos aplicativos”); • Atualização de referências.
05/07/2021	3.3	• Criação da nova seção 6, intitulada “Implementação segura de aplicativos, *APIs* e outros sistemas”.

29/10/2021	3.4	• Alteração da seção 5 “Certificados digitais” para prever a transição para o novo padrão do certificado de autenticação e criptografia da conexão utilizado pelo BC e mudança no procedimento de desativação do certificado dos participantes. • Ajustes de redação para maior clareza.
16/11/2022	3.5	• Ajustes na seção de certificados digitais – itens 5.1, 5.4.3, 5.4.4 e 5.5. • Ajustes na seção 6 – alteração dos itens 1 e 5, inclusão do item 7 e outras pequenas alterações.
19/01/2024	3.6	• Inclusão (seção 5.2) de prazo regulamentar para atualização de certificados digitais. • Ajustes de redação para enfatizar a obrigatoriedade da adequada guarda de chaves criptográficas privadas e de boas práticas de gestão de certificados e chaves (seção 5.2 e 5.3). • Ajustes de redação para maior clareza.

Apresentação

Este manual descreve os principais requisitos técnicos de segurança do ecossistema de pagamentos instantâneos (Pix), e tem como objetivo descrever como deve ser implementada a criptografia da comunicação, a autenticação, os processos de assinatura digital e de gestão dos certificados digitais utilizados no ecossistema, bem como os aspectos de segurança associados à iniciação de pagamentos por *QR Codes* dinâmicos. Os requisitos para implementação segura de aplicativos, APIs e sistemas relacionados ao Pix também constam neste manual, assim como os requisitos para manutenção de logs de auditoria.

Referências

Estas especificações baseiam-se, referenciam, e complementam onde aplicável, os seguintes documentos:

Referência	Origem
Resolução BCB nº 1 (Regulamento do Pix)	https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=1
Manual de Segurança do SFN	https://www.bcb.gov.br/estabilidadefinanceira/comunicacaodados
Manual de Redes do SFN	https://www.bcb.gov.br/estabilidadefinanceira/comunicacaodados
Catálogo de Serviços do SFN	https://www.bcb.gov.br/estabilidadefinanceira/comunicacaodados
Manual das Interfaces de Comunicação	https://www.bcb.gov.br/estabilidadefinanceira/comunicacaodados
Diretório de Identificadores de Contas Transacionais (DICT)	https://www.bcb.gov.br/estabilidadefinanceira/pix
Padrões para Iniciação do Pix	https://www.bcb.gov.br/estabilidadefinanceira/pix
Sistema de Transferência de Arquivos do Banco Central (STA)	https://www.bcb.gov.br/estabilidadefinanceira/pix
Aplicação BC Correio	https://bccorreio.bcb.gov.br/bccorreio/
ICP-Brasil	https://www.iti.gov.br/icp-brasil
ISO 20.022	https://www.iso20022.org/
XML Signature Syntax and Processing (Second Edition)	https://www.w3.org/TR/2008/REC-xmldsig-core-20080610/
Padrão de assinatura digital *JSON Web Signature (JWS) – RFC* 7515	https://tools.ietf.org/html/rfc7515
JSON Web Key – RFC 7517	https://tools.ietf.org/html/rfc7517
JSON Web Algorithms (JWA) – RFC 7518	https://tools.ietf.org/html/rfc7518
Padrão de certificados X.509 – *RFC* 5280	https://tools.ietf.org/html/rfc5280
Well-Known URIs – RFC 8615	https://tools.ietf.org/html/rfc8615
Good Practices for Capability URLs	https://www.w3.org/TR/capability-urls/ - ver o último draft, disponível em: https://w3ctag.github.io/capability-urls/.
Randomness Recommendations for Security – RFC 4086	https://tools.ietf.org/html/rfc4086
A Universally Unique IDentifier (UUID) URN Namespace – RFC 4122	https://tools.ietf.org/html/rfc4122
OCSP – Online Certificate Status Protocol – RFC 6960	https://tools.ietf.org/html/rfc6960
Lei Geral de Proteção de Dados (LGPD)	http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Sugestões, críticas ou pedidos de esclarecimento de dúvidas podem ser enviados ao BC por meio do e-mail pix@bcb.gov.br.

1.Introdução

A segurança é um elemento primordial do Pix e, para garanti-la, requisitos importantes devem ser estabelecidos e diversos controles devem ser colocados em prática, não só pelo Banco Central, mas por todos os participantes do ecossistema. Nesse contexto, é necessário implementar criptografia e autenticação mútua na comunicação entre os participantes e as *API*s do Pix e as mensagens transmitidas no âmbito do sistema devem ser assinadas digitalmente. A iniciação de pagamentos, em especial quando ocorre por meio de *QR Codes* dinâmicos, também possui aspectos de segurança importantes que devem ser considerados. Ademais, logs de auditoria devem ser mantidos pelas instituições no intuito de prover a rastreabilidade das mensagens e transações realizadas no Pix.

Este documento apresenta os detalhes técnicos associados aos requisitos de segurança a serem adotados nas diferentes *API*s e tecnologias que compõem o Pix. Para outras informações sobre o Pix, incluindo a definição de alguns termos utilizados neste documento, como "participante" e "prestador de serviços de pagamento" (PSP), verificar o Regulamento do Pix, anexo à Resolução BCB Nº 1, de 12 de agosto de 2020[1].

[1] Resolução BCB Nº 1, de 12 de agosto de 2020 – disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=1.

2. Comunicação segura

A comunicação entre cada participante e o Pix é realizada por meio da Rede do Sistema Financeiro Nacional (RSFN). A conexão do participante com a RSFN deve observar as regras e padrões dispostos no Manual de Redes do SFN[2].

O participante deve se conectar às *APIs* disponíveis no Pix exclusivamente por meio do protocolo *HTTP* versão 1.1 utilizando criptografia *TLS* versão 1.2 ou superior, com autenticação mútua obrigatória no estabelecimento da conexão. Deve ser suportada, no mínimo, a *Cipher Suite ECDHE-RSA-AES-128-GCM-SHA256 (0xc02f)*, ou seja, os seguintes algoritmos devem ser utilizados:

Fase/Função	Algoritmo
Troca de chaves	*ECDHE (Elliptic Curve Diffie Hellman Ephemeral)*
Autenticação	*RSA*
Criptografia simétrica	*AES* com chaves de 128 *bits* utilizando o modo *GCM*
MAC (Message Authentication Code)	*SHA* de 256 *bits*

Tabela 1: Algoritmos utilizados na criptografia TLS.

As informações sobre os certificados a serem utilizados para autenticação e criptografia da comunicação constam na seção 5 deste documento.

Os clientes *HTTP* do participante devem sempre respeitar o *TTL* (*Time To Live*) dos servidores *DNS*. A falha em respeitar o *TTL* pode causar indisponibilidade no acesso às *APIs* do Pix.

[2] Manual de Redes do SFN – última versão disponível na página: https://www.bcb.gov.br/estabilidadefinanceira/comunicacaodados.

3. Assinatura digital

No intuito de garantir a integridade e o não repúdio das transações no âmbito do Pix, todas as mensagens trafegadas no Sistema de Pagamentos Instantâneos (SPI) devem ser assinadas digitalmente pelo emissor. No caso do Diretório de Identificadores de Contas Transacionais (DICT)[3], apenas as requisições de consulta (*GET*) não precisam ser assinadas, enquanto todas as demais requerem assinatura. Seja qual for a operação realizada, tanto no SPI como no DICT, a resposta do BC para o participante é sempre assinada.

O padrão de assinatura digital a ser utilizado no Pix é o *XMLDSig*[4]. No SPI, as mensagens seguem o padrão *ISO* 20.022[5], portanto a assinatura digital deve constar no elemento <*Sgntr*> do *Business Application Header (BAH)*[6], conforme descrito no Catálogo de Serviços do SFN[7]. No DICT, por sua vez, as requisições e respostas não são realizadas por meio de mensagens *ISO 20.022*, então o cabeçalho (*BAH*) não existe. Nesse caso, a assinatura (elemento <*Signature*>) deve constar na raiz do *XML*.

A tabela abaixo mostra os elementos/*tags* que devem compor a assinatura digital:

#	Elemento/*tag*	Descrição
1	<*Signature*>	Elemento raiz da assinatura *XMLDSig*, onde se define o *namespace*, que aponta para a *URI* do esquema *XML* (*XML Schema Definition – XSD*) a ser utilizado para a assinatura digital. Inclui todos os elementos descritos nas demais linhas desta tabela. No Pix, é utilizado *XMLDSig*: http://www.w3.org/2000/09/xmldsig#
1.1	<*SignedInfo*>	Contém as principais informações necessárias para a assinatura, e inclui as *tags* <*CanonicalizationMethod*>, <*SignatureMethod*> e *tags* <*Reference*>, descritas abaixo.
1.1.1	<*CanonicalizationMethod*>	Especifica o algoritmo de canonicalização a ser aplicado no elemento <*SignedInfo*>, com o objetivo de gerar a forma canônica do conteúdo a partir do qual será gerado o resumo *(digest)* para posterior assinatura digital. No Pix, deve ser utilizado o algoritmo de canonicalização *XML* exclusiva: http://www.w3.org/2001/10/xml-exc-c14n#.

[3] A *API* do DICT é documentada em manual específico, cuja última versão está disponível na página: https://www.bcb.gov.br/estabilidadefinanceira/pix.

[4] *W3C Recommendation – XML Signature Syntax and Processing (Second Edition)*, disponível em: https://www.w3.org/TR/2008/REC-xmldsig-core-20080610/

[5] Padrão *ISO* 20.022 – mais informações disponíveis em: https://www.iso20022.org/

[6] Mais detalhes sobre o *BAH* podem ser obtidos na página da ISO 20.022 (ver referência anterior).

[7] Catálogo de Serviços do SFN – última versão disponível em https://www.bcb.gov.br/estabilidadefinanceira/comunicacaodados.

1.1.2	*<SignatureMethod>*	Define o algoritmo utilizado para geração e validação da assinatura digital. No Pix, utiliza-se *RSA-SHA256*: http://www.w3.org/2001/04/xmldsig-more#rsa-sha256.
1.1.3	*<Reference>*	Elemento que referencia o conteúdo a ser assinado, e inclui as *tags* *<Transforms>*, *<DigestMethod>* e *<DigestValue>*. A utilização do elemento *<Reference>* é detalhada na seção 3.1 a seguir.
1.1.3.1	*<Transforms>*	Inclui uma ou mais *tags* *<Transform>*, que indicam que transformações devem ser aplicadas, sempre em sequência, no conteúdo a partir do qual será gerado o resumo (*digest*). As transformações realizadas constam nas tabelas 3 e 4 da seção 3.1.
1.1.3.2	*<DigestMethod>*	Identifica qual algoritmo de *digest* será aplicado ao conteúdo a ser assinado. No Pix, utiliza-se *SHA-256*: http://www.w3.org/2001/04/xmlenc#sha256.
1.1.3.3	*<DigestValue>*	Elemento que contém o resumo (*digest*) codificado em *base64*.
1.2	*<KeyInfo>*	Elemento que contém os dados do certificado utilizado para assinar digitalmente o conteúdo. Inclui a *tag* *<X509Data>*, explicada abaixo.
1.2.3	*<X509Data>*	Contém os dados do certificado *X509* utilizado pelo assinador. Inclui a *tag* *<X509IssuerSerial>*, descrita abaixo.
1.2.3.1	*<X509IssuerSerial>*	Contém as *tags* *<X509IssuerName>* e *<X509SerialNumber>*, descritas abaixo.
1.2.3.1.1	*<X509IssuerName>*	Contém o nome (*Distinguished Name – DN*) da AC que gerou o certificado utilizado para assinatura digital.
1.2.3.1.2	*<X509SerialNumber>*	Contém o número de série do certificado utilizado para assinatura digital.
1.3	*<SignatureValue>*	Elemento que contém a assinatura digital propriamente dita, codificada em *base64*.

Tabela 2: Elementos que compõem a assinatura digital no Pix.

3.1. Informações a serem assinadas

No SPI, as informações a serem assinadas são:

- Mensagem *ISO 20.022* (elemento *<Document>*);
- Cabeçalho – *BAH* (elemento *<AppHdr>*);
- Elemento *<KeyInfo>*.

Portanto, no SPI são utilizados 3 elementos *<Reference>*, como mostra a tabela 3:

Tag	Conteúdo referenciado	Transformações a serem realizadas
<Reference URI="<unique-id-to-KeyInfo>	*<KeyInfo Id="unique-id-to-KeyInfo">* *(.....)* *</KeyInfo>*	Canonicalização *XML* Exclusiva: http://www.w3.org/2001/10/xml-exc-c14n#
<Reference URI ="">	*BAH* (excluindo os elementos da assinatura digital)*:* *<AppHdr>* *(.....)* *</AppHdr>*	*XMLDSig Enveloped Signature*: http://www.w3.org/2000/09/xmldsig#enveloped-signature e Canonicalização *XML* Exclusiva: http://www.w3.org/2001/10/xml-exc-c14n#
<Reference>	*<Document>* *(.....)* *</Document>*	Canonicalização XML Exclusiva: http://www.w3.org/2001/10/xml-exc-c14n#

Tabela 3: Elementos <Reference> utilizados no SPI, bem como as transformações realizadas.

Observação: no SPI, a tag <Reference>, sem o atributo URI, deve ser interpretada pela aplicação de forma a referenciar a mensagem ISO 20.022 propriamente dita (elemento <Document>).

Já no caso do DICT, é necessário assinar o conteúdo do elemento raiz do *XML* e do *<KeyInfo>*, o que resulta na utilização de apenas 2 *tags <Reference>*, conforme mostrado na tabela abaixo:

Tag	Conteúdo referenciado	Transformações a serem realizadas
<Reference URI="<unique-id-to-KeyInfo>	*<KeyInfo Id="unique-id-to-KeyInfo">* *(.....)* *</KeyInfo>*	Canonicalização *XML* Exclusiva: http://www.w3.org/2001/10/xml-exc-c14n#
<Reference URI ="">	*<Elemento-raiz-do-XML>* *(.....)* *</Elemento-raiz-do-XML>*	*XMLDSig Enveloped Signature*: http://www.w3.org/2000/09/xmldsig#enveloped-signature e Canonicalização *XML* Exclusiva: http://www.w3.org/2001/10/xml-exc-c14n#

Tabela 4: Elementos <Reference> utilizados no DICT, bem como as transformações realizadas.

Observação: ressalta-se que, no caso do DICT, a tag <Reference URI =""> aponta para a raiz do XML, diferentemente do que ocorre no SPI.

3.2. Processo de assinatura digital

No SPI, o processo de assinatura digital das mensagens inclui os passos abaixo:

1. Obter a mensagem completa a ser assinada;
2. Construir o elemento *<KeyInfo>*, incluindo as informações sobre o certificado digital utilizado na assinatura, conforme item 1.2 e subitens da tabela 2;
3. Extrair *BAH* (*tag <AppHdr>*);
4. Extrair mensagem *ISO 20.022* (*tag <Document>*);
5. No elemento *<SignedInfo>*, definir o algoritmo de canonicalização e de assinatura digital a serem utilizados, conforme itens 1.1.1 e 1.1.2 da tabela 2;
6. Criar os elementos *<Reference>*, incluindo as *tags <Transforms>* e *<Transform>* conforme tabela 3 e item 1.1.3 e subitens da tabela 2;

7. Efetuar as transformações nos conteúdos, conforme tabela 3;
8. Gerar os *digests* para os conteúdos referenciados nos itens acima, incluindo-os nos respectivos elementos <*DigestValue*>;
9. Canonicalizar o elemento <*SignedInfo*> e assiná-lo digitalmente conforme algoritmos definidos no passo 5 acima;
10. Inserir a assinatura digital gerada no passo anterior no elemento <*SignatureValue*>.

A figura na página a seguir ilustra o processo de assinatura no SPI:

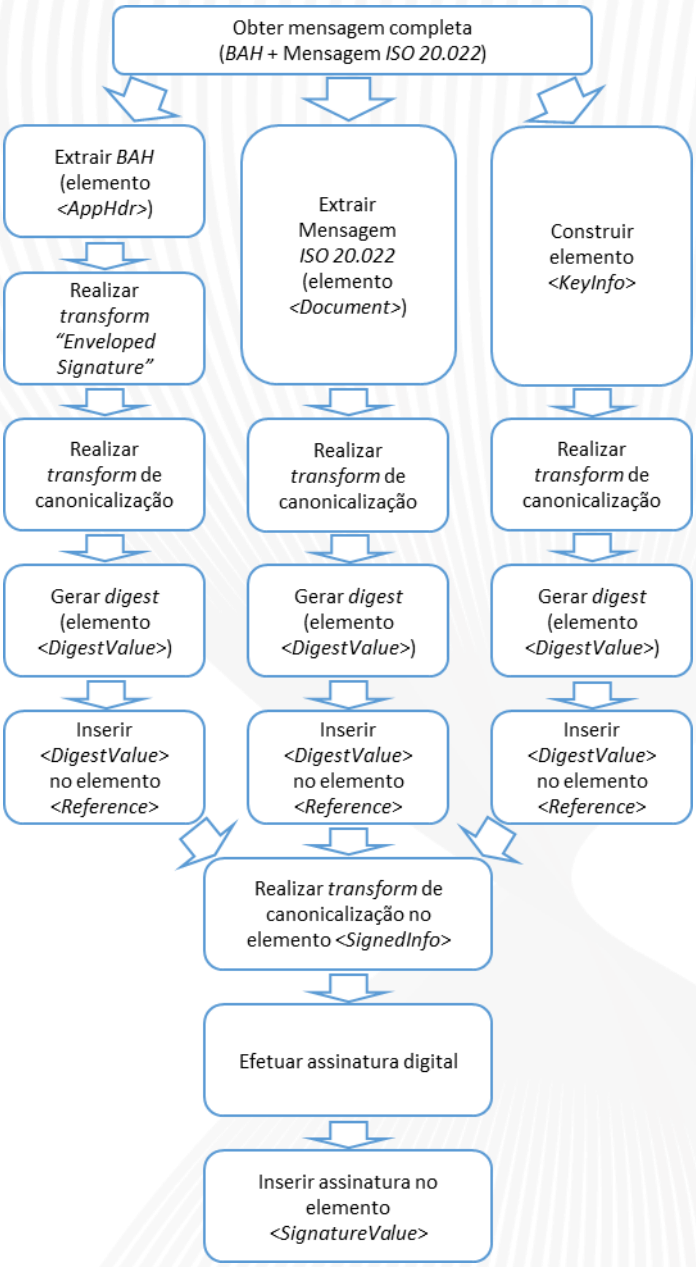

Figura 1 – Fluxo de assinatura digital da mensagem no SPI.

A seguir consta um exemplo de mensagem *pacs.008* assinada digitalmente:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<Envelope xmlns="https://www.bcb.gov.br/pi/pacs.008/1.4">
 <AppHdr>
  (...)
  <Sgntr>
   <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
     <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
     <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
     <ds:Reference URI="#key-info-id">
      <ds:Transforms>
       <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <ds:DigestValue>J9fL+QyrtblrJnk0gjGnGPaDt42AKfNRM3uv4EbdbrM=</ds:DigestValue>
     </ds:Reference>
     <ds:Reference URI="">
      <ds:Transforms>
       <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
       <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <ds:DigestValue>D8tkpivJTLnU5YQt8E9T/723ykNv1h41qu07hnIwV+4=</ds:DigestValue>
     </ds:Reference>
     <ds:Reference>
      <ds:Transforms>
       <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <ds:DigestValue>B/xG0ETsGoVLZtgbdvPtfHMYJORIpEzkBPTWfL1gMbI=</ds:DigestValue>
     </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>
QfbSxaFsYZ89+EkweSWRcoP9hcam3NFwr2gwrbK50XZdZJA/DqaH6icqU/Ys2AHwR78KNx1LVqpg
J6bdVg4kDYu9PAoWzCcRLBJb6gRlSchyR7Uaih2PnNfaJ+OU7YREJW391d5hGds0F/ufNpVc2r6+
9DrYvxcphC9YKKb7v0Qw7Jyj13TimghPsqH1XTxeKHmby+MU7aObksTHBXgpEIMezsZhPOG5LNqT
Kq1e3tiQQvseHW6qO8rcHtIeI/Q9jtw+Idipwhu7lbS2XvoOcdHf2LWlQo6Tm77PJVvkJaQTd8tw
iUwaQkubtWuoGmUB4blYafy5Sby1OjZR5EAaMg==
    </ds:SignatureValue>
    <ds:KeyInfo Id="key-info-id">
     <ds:X509Data>
      <ds:X509IssuerSerial>
       <ds:X509IssuerName>CN=AC Exemplo, OU=CSPB-0, O=ICP-Brasil, C=BR</ds:X509IssuerName>
       <ds:X509SerialNumber>20200130224837516000</ds:X509SerialNumber>
      </ds:X509IssuerSerial>
     </ds:X509Data>
    </ds:KeyInfo>
   </ds:Signature>
  </Sgntr>
 </AppHdr>
 <Document>
  (...)
 </Document>
</Envelope>
```

Observação: trechos do XML não relacionados à assinatura foram cortados e estão representados com (...). Mais informações sobre o XML como um todo constam no Catálogo de Serviços do SFN.

No DICT, por sua vez, o processo de assinatura digital inclui os passos abaixo:

1. Obter o conteúdo do elemento raiz do *XML* a ser assinado;
2. Construir o elemento <*KeyInfo*>, incluindo as informações sobre o certificado digital utilizado na assinatura, conforme item 1.2 e subitens da tabela 2;
3. No elemento <*SignedInfo*>, definir o algoritmo de canonicalização e de assinatura digital a serem utilizados, conforme itens 1.1.1 e 1.1.2 da tabela 2;
4. Criar os elementos <*Reference*>, incluindo as *tags* <*Transforms*> e <*Transform*> conforme tabela 4 e item 1.1.3 e subitens da tabela 2;
5. Efetuar as transformações nos conteúdos, conforme tabela 4;
6. Gerar os *digests* para os conteúdos referenciados nos itens acima, incluindo-os nos respectivos elementos <*DigestValue*>;
7. Canonicalizar o elemento <*SignedInfo*> e assiná-lo digitalmente conforme algoritmos definidos no passo 3 acima;
8. Inserir a assinatura digital gerada no passo anterior no elemento <*SignatureValue*>.

A figura na página a seguir ilustra o processo de assinatura no DICT:

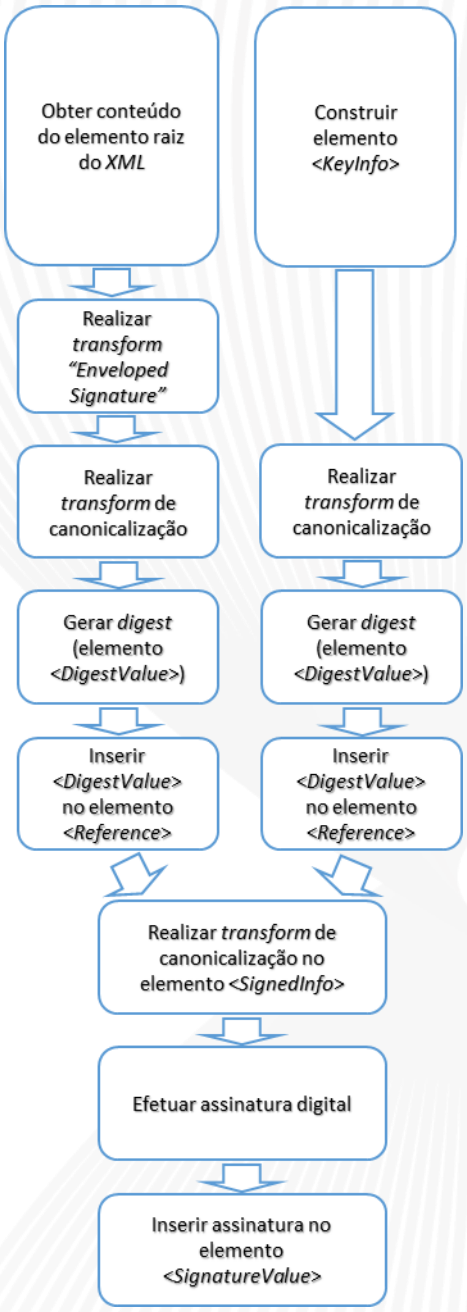

Figura 2 – Fluxo de assinatura digital no DICT.

3.3. Verificação da assinatura digital

No SPI, o processo de verificação da assinatura digital das mensagens inclui os passos abaixo:

1. Extrair o elemento <*KeyInfo*> da assinatura (*tag* <*Signature*>);
2. Extrair a mensagem *ISO 20.022* (*tag* <*Document*>);
3. Extrair o *BAH* (*tag* <*AppHdr*>*)* e aplicar o *transform "Enveloped Signature"*;
4. Canonicalizar o resultado dos 3 passos acima;
5. Gerar o *digest* dos 3 resultados obtidos no passo anterior;
6. Comparar os *digests* gerados com os valores dos campos <*DigestValue*> que constam nos respectivos elementos <*Reference*>;
7. Caso a verificação seja bem sucedida, proceder com os passos abaixo. Caso contrário, retornar erro.
8. Obter a assinatura digital da mensagem (elemento <*SignatureValue*>);
9. A partir das informações constantes no elemento <*KeyInfo*>, obter certificado do emissor (*);
10. Canonicalizar elemento <*SignedInfo*>;
11. Verificar a assinatura obtida no passo 8 utilizando a chave pública do certificado obtido no passo 9 acima para confirmá-la.
12. Caso a verificação seja bem sucedida, finalizar processo com status de sucesso. Caso contrário, retornar erro.

(*) Cada participante é responsável por manter uma base atualizada com os números de série e respectivas chaves públicas dos certificados digitais do BC utilizados para assinatura digital. O BC ativará seus certificados conforme descrito na seção 5.4.

A figura na página a seguir ilustra o processo:

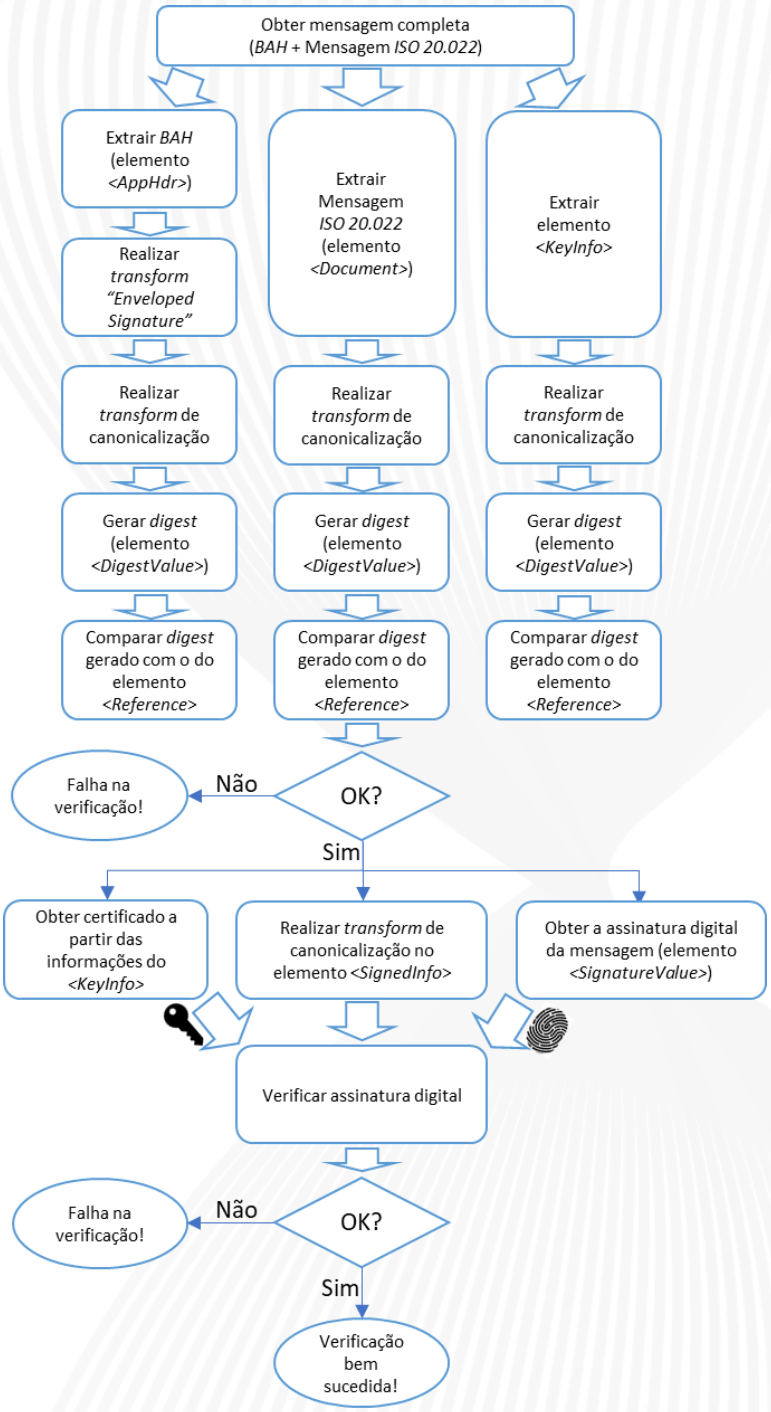

Figura 3 – Fluxo de verificação da assinatura digital da mensagem no SPI.

Já no DICT, o processo de verificação da assinatura digital consiste nos seguintes passos:

1. Obter o conteúdo do elemento raiz do *XML*;
2. Aplicar o *transform "Enveloped Signature"* no conteúdo;
3. Extrair o elemento <*KeyInfo*> da assinatura (*tag* <*Signature*>);
4. Canonicalizar o resultado dos passos 2 e 3 acima;
5. Gerar o *digest* dos 2 resultados obtidos no passo anterior;
6. Comparar os *digests* gerados com os valores dos campos <*DigestValue*> que constam nos respectivos elementos <*Reference*>;
7. Caso a verificação seja bem sucedida, proceder com os passos abaixo. Caso contrário, retornar erro.
8. Obter a assinatura digital (elemento <*SignatureValue*>);
9. A partir das informações constantes no elemento <*KeyInfo*>, obter certificado do emissor;
10. Canonicalizar elemento <*SignedInfo*>;
11. Verificar a assinatura obtida no passo 8 utilizando a chave pública do certificado obtido no passo 9 acima para confirmá-la.
12. Caso a verificação seja bem sucedida, finalizar processo com status de sucesso. Caso contrário, retornar erro.

A figura na página a seguir ilustra o processo:

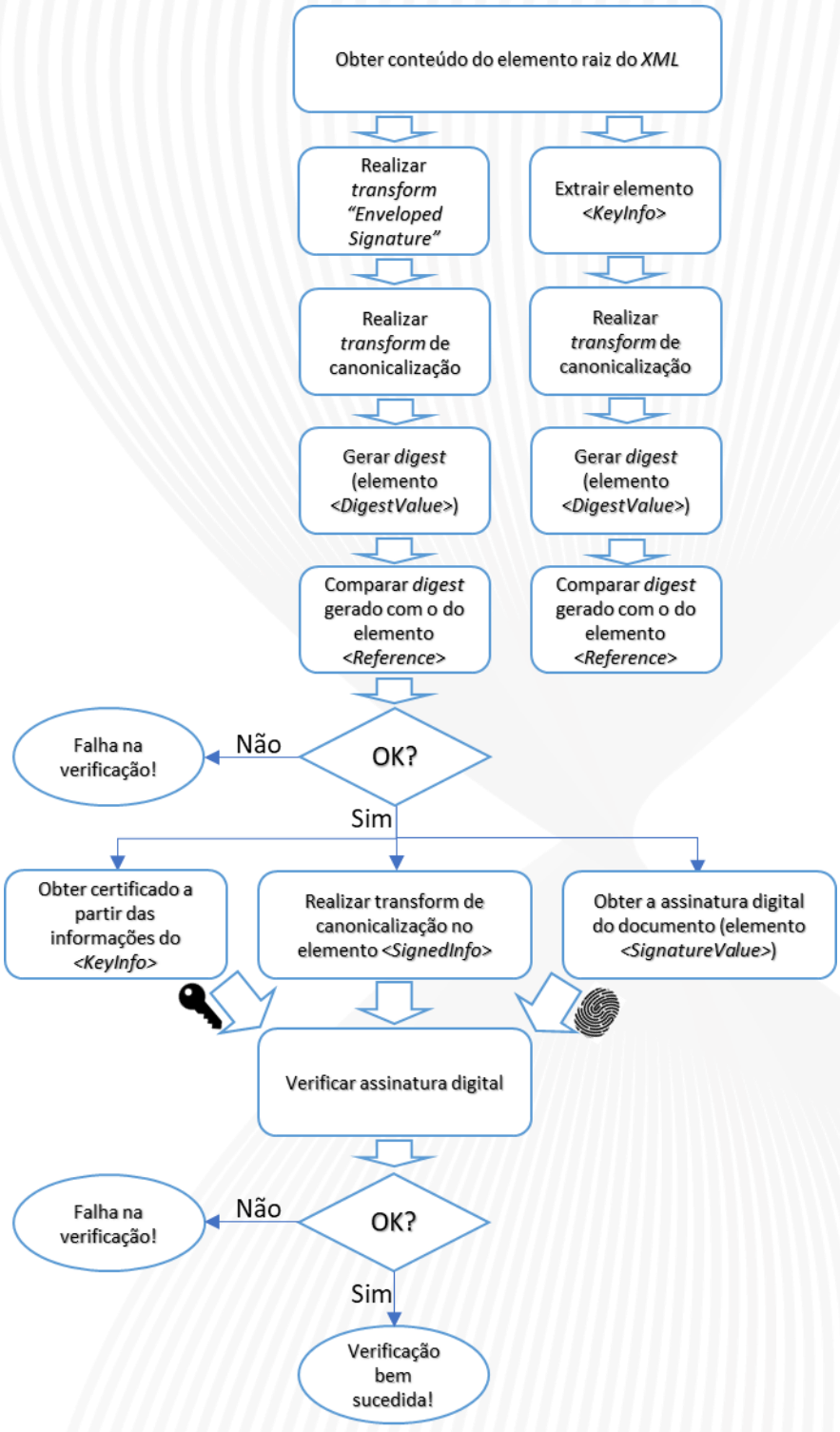

Figura 4 – Fluxo de verificação da assinatura digital no DICT.

4. Segurança de *QR Codes* dinâmicos

Esta seção apresenta as especificações de segurança de *QR Codes* dinâmicos gerados pelo recebedor.

Conforme especificado no Manual de Padrões para Iniciação do Pix[8], o *QR Code* dinâmico gerado pelo recebedor contém, dentre outras informações, uma *URL* que é acessada de forma criptografada no momento de sua leitura. O conteúdo acessado consiste em uma estrutura *JWS (JSON Web Signature)*[9] cujo *payload*, assinado digitalmente, contém informações da transação. Os detalhes a respeito da segurança no acesso às *URLs*, certificados e processo de assinatura digital constam a seguir.

4.1. Segurança no acesso às *URLs*

A *URL* acessada ao se efetuar a leitura de um *QR Code* dinâmico deve ser provida pelo PSP recebedor em site que implemente o protocolo *HTTPS* com criptografia *TLS* versão 1.2 ou superior. O PSP recebedor deve ser proprietário do site/domínio – ou, caso contrate provedor de serviços para essa finalidade, o PSP deve se responsabilizar pela segurança e disponibilidade do site.

Como medida adicional de segurança, além dos requisitos obrigatórios acima, recomenda-se que cada PSP crie e mantenha registros *CAA ("Certification Authority Authorization")*[10] no *DNS* do domínio que hospeda os sites relacionados a *QR Codes* dinâmicos.

A *URL* presente no *QR code* dinâmico não deve incluir prefixo de protocolo, uma vez que este deve ser sempre *HTTPS*, conforme já especificado no início desta seção. Respeitadas as regras de formação de *URL*[11] e as definições do Manual do BR Code[12], os seguintes componentes devem estar presentes:

fqdnPspRecebedor/pixEndpoint/pixUrlAccessToken/

O tamanho máximo da *URL* completa (sem o prefixo de protocolo) deve ser 77 caracteres e o domínio do recebedor na *URL* deve ser completamente qualificado

[8] Manual de Padrões para Iniciação do Pix" – última versão disponível na página: https://www.bcb.gov.br/estabilidadefinanceira/pix.
[9] Padrão de assinatura digital *JSON Web Signature (JWS)*, definido pela *RFC* 7515, disponível em https://tools.ietf.org/html/rfc7515.
[10] DNS CAA (Certificate Authority Authorization, disponível em https://tools.ietf.org/html/rfc6844.
[11] A sintaxe, a semântica e outros aspectos a respeito de *URLs* são definidas pela *RFC* 1738, disponível em https://tools.ietf.org/html/rfc1738.
[12] Conforme estabelecido pela Carta Circular 4.014/2020, disponível em https://www.bcb.gov.br/estabilidadefinanceira/arranjosintegrantesspb.

(*FQDN*). O *endpoint*/aplicação do recebedor é opcional, mas, se presente, deve ser respeitado.

***pixURLAccessToken*: aleatoriedade e segurança**

O componente da *URL* denominado "*pixUrlAccessToken"* é um identificador único que serve para evitar varreduras de "força bruta" por outros agentes que não tenham acesso ao *QR Code*, viabilizando a leitura dos detalhes de pagamento (*payload JSON*) apenas para o pagador[13]. O *pixUrlAccessToken* deve respeitar as seguintes restrições:

- Tamanho mínimo de 120 *bits* aleatórios;
- Tamanho máximo conforme disponível, considerando os demais componentes da *URL*;
- Não deve ser possível deduzir seu valor, exceto pela leitura do *QR Code*, conforme detalhado abaixo.

Para impedir a dedução do *pixUrlAccessToken* por terceiros, o PSP recebedor deve criá-lo conforme as recomendações do documento do *W3C* intitulado "*Good Practices for Capability URLs*"[14], além de considerar aspectos que garantam alto grau de entropia e de aleatoriedade – ver *RFC* 4086 ("*Randomness Requirements for Security*")[15]. Uma abordagem possível é utilizar o padrão *UUID*[16] v4 para representar o *pixUrlAccessToken*, desde que o algoritmo utilizado para gerá-lo atenda ao requisito de aleatoriedade real. É importante frisar que o uso da versão 4 é obrigatório caso se opte por esse padrão, pois ela é a única em que o *UUID* é gerado com valores aleatórios.

O pagador não efetua validações no *pixUrlAccessToken*, sendo responsabilidade do PSP recebedor garantir suas propriedades mínimas de segurança.

Caso um PSP deseje implementar site para *QR Codes* em ambiente de homologação, o nome do servidor ("*host*") do site deverá, obrigatoriamente, terminar com "*-h*" – exemplo: "*qrcode-h.bancoxyz.com.br*". No caso dos sites para *QR Codes* de produção, a única restrição é que o nome do *host* não deve terminar com "*-h*".

4.2. Definições do padrão *JWS*

Conforme já mencionado, ao se efetuar a leitura de um *QR Code* dinâmico gerado pelo recebedor, será acessada uma *URL* cujo conteúdo consiste em uma estrutura *JWS* em

[13] A *URL* estará exposta a qualquer agente que tenha acesso ao *QR Code* gerado.
[14] *W3C – "Good Practices for Capability URLs"*, disponível em https://www.w3.org/TR/capability-urls/. Ver o último *draft*, que consta em: https://w3ctag.github.io/capability-urls/.
[15] *RFC* 4086 ("*Randomness Requirements for Security"*), disponível em https://tools.ietf.org/html/rfc4086, apresenta as melhores práticas para geração de dados aleatórios.
[16] *RFC* 4122 ("*A Universally Unique IDentifier (UUID) URN Namespace*"), disponível em: https://tools.ietf.org/html/rfc4122.

que o *payload* é assinado digitalmente pelo PSP recebedor, para garantir a integridade e não-repúdio das informações da transação. A estrutura *JWS* inclui:

- Cabeçalho (*JSON Object Signing and Encryption – JOSE Header*), onde se define o algoritmo utilizado e inclui informações sobre a chave pública ou certificado que podem ser utilizadas para validar a assinatura;
- *Payload* (*JWS Payload*): conteúdo propriamente dito;
- Assinatura digital (*JWS Signature*): assinatura digital, realizada conforme parâmetros do cabeçalho.

Cada elemento acima deve ser codificado utilizando o padrão *Base64url*[17] e, feito isso, os elementos devem ser concatenados com *"."* (método *JWS Compact Serialization*, conforme definido na *RFC* 7515).

No contexto do Pix, o cabeçalho (*JOSE Header*) deve incluir no mínimo os parâmetros abaixo:

- *"alg" (Algorithm)*: algoritmo de assinatura digital utilizado.
  - Valores proibidos: "*HS**" *(*relacionados a *HMAC)* e *"none"*.
  - Valores permitidos: "*RS256"* ou superior e "*ES256"* ou superior.
  - Valores recomendados: "*PS256"* ou "*PS512"*.
- *"x5t" (X.509 Certificate SHA-1 Thumbprint)* (*): *thumbprint*, codificado em *Base64url*, do certificado que corresponde à chave privada utilizada para assinatura do *JWS*.
  (*) Alternativamente, poderá ser utilizado o parâmetro *x5t#S256* (*X.509 Certificate SHA-256 Thumbprint*) ou superior, de acordo com a função *hash* utilizada para gerar o *thumbprint*.
- *"jku" (JWK Set URL)*: *URL* onde consta um conjunto de chaves no formato *JSON (JWK Set*[18]*).*
  - A *URL* deve estar hospedada no mesmo site associado ao certificado *CERTQRC* cadastrado conforme descrito na seção 5.2.
- *"kid" (Key ID)*: Identificador da chave a ser utilizada para validar a assinatura digital, dentre as chaves presentes no *JWK Set* acessado por meio da *URL* definida no parâmetro "*jku"*.

O *JWK Set* disponível na *URL* acima deve incluir o parâmetro *keys*, cujo valor consiste em uma ou mais chaves no padrão *JWK*, conforme definido na *RFC* 7517. A estrutura *JWK*, por sua vez, deve incluir no mínimo os parâmetros abaixo:

- *"kty" (Key Type)*: algoritmo criptográfico da chave.
  - Deve ser "*RSA"* (*) ou *"EC"* (**).

[17] As definições sobre o padrão Base64url constam na seção 5 da *RFC* 4648, disponível em https://tools.ietf.org/html/rfc4648#section-5.
[18] A estrutura *JSON Web Key* é definida pela *RFC* 7517, disponível em https://tools.ietf.org/html/rfc7517.

(*) Neste caso, também devem ser inclusos no *JWK* os parâmetros abaixo:

- "*n*": módulo da chave pública *RSA*;
- "*e*": expoente da chave.

(**) Neste caso, também devem ser inclusos no *JWK* os parâmetros que definem a curva elíptica utilizada:

- "*crv*": identificador da curva criptográfica utilizada;
  - Valores permitidos: "*P-256*", "*P-384*" e "*P-521*".
- "x": coordenada X do ponto da curva elíptica;
- "y": coordenada Y do ponto da curva elíptica.

- "*key_ops" (Key Operations)*: operação para a qual a chave deve ser utilizada.
  - Deve ser sempre "*verify*", pois a chave será usada para verificar a assinatura digital do *JWS*.
- *"kid" (Key ID)*: Identificador único da chave no *JWK Se*t.
- *"x5t" (X.509 Certificate SHA-1 Thumbprint)* (*): *thumbprint*, codificado em *Base64url*, do certificado que corresponde à chave privada utilizada para assinatura do *JWS*.

  (*) Alternativamente, poderá ser utilizado o parâmetro *x5t#S256* (*X.509 Certificate SHA-256 Thumbprint*) ou superior, de acordo com a função *hash* utilizada para gerar o *thumbprint*.
- *"x5c" (X.509 Certificate Chain*): certificado digital *X.509*, contendo a chave pública que corresponde à chave privada utilizada na assinatura digital, bem como sua respectiva cadeia completa de certificação, incluindo o certificado da AC raiz.
  - Deve-se utilizar um *array JSON* com os certificados, começando com o certificado cuja chave privada correspondente foi utilizada na assinatura, seguido pelo certificados adicionais da cadeia, onde cada certificado subsequente tenha sido utilizado para emissão do certificado anterior, conforme exemplo do *Appendix B* da *RFC* 7515.
  - Assim como no caso do certificado associado ao site que hospeda a estrutura *JWS*, o certificado neste caso deve ser válido e emitido por AC amplamente conhecida.

Os parâmetros "*x5t*" e "*kid*" definidos no *JWK Set* devem corresponder aos parâmetros de mesmo nome que constam no cabeçalho *JWS*, permitindo que a aplicação cliente consiga identificar de maneira inequívoca o certificado e a chave pública a ser utilizada para verificar a assinatura digital do *JWS*.

Mais informações sobre os parâmetros do *JWS* e *JWK Set* constam na *RFC* 7518[19], além das *RFCs* 7515 e 7517 já citadas anteriormente.

[19] *RFC* 7518 – "*JSON Web Algorithms (JWA)*", disponível em https://tools.ietf.org/html/rfc7518.

4.3. Validações a serem feitas pelos aplicativos

Após efetuar a leitura de um *QR Code* dinâmico, os aplicativos de cada participante devem seguir os passos abaixo:

- Verificar se a *URL* que consta no *QR Code* é hospedada em site com criptografia *TLS* versão 1.2 ou superior, conforme seção 4.1;
- Verificar se o certificado associado ao site está cadastrado no Pix, conforme seção 5.2, e efetuar as demais validações do certificado e respectiva cadeia de certificação;
- Verificar se o site consta no campo *CN* (*"Common Name"*) ou *SAN* (*"Subject Alternative Name"*) do certificado;
- Obter a chave pública e o certificado associado conforme informações do cabeçalho *JWS* e *JWK Set*;
- Validar o certificado obtido no passo anterior, bem como sua cadeia de certificação, conforme definido na *RFC* 5280[20];
- Validar a assinatura digital (*JWSSignature*) com a chave pública obtida anteriormente;
- Se e somente se a assinatura estiver válida, o aplicativo deve processar os dados do *payload JSON* e realizar a transação;
- Caso o nome do servidor ("*host*") do site/*URL* relacionado ao *QR Code* termine com "*-h*", um aplicativo de produção não deve proceder com a transação, uma vez que esse site/*URL* só deve ser usado em ambiente de homologação.

Cabe aos participantes implementarem mecanismos em seus aplicativos para otimizar o processo de verificação da assinatura digital do *JWS*. Por exemplo, é possível que o aplicativo armazene previamente um conjunto de *thumbprints* de certificados e suas respectivas chaves públicas de forma que, ao ler o parâmetro *x5t* do *JWS*, o aplicativo já consiga saber qual chave utilizar para validar a assinatura digital, sem precisar acessar a *URL* definida no parâmetro *jku*.

Recomenda-se que, para facilitar esse processo de "carga prévia" de *thumbprints* e chaves públicas nos aplicativos, cada PSP mantenha um diretório "*/.well-known/*"[21] no seu site associado a *QR Codes* dinâmicos. Tal diretório pode conter, por exemplo, um documento *host-meta*[22] que especifique as *URLs* dos seus *JWK Sets* (parâmetro *jku* do *JWS*). Assim, os demais participantes conseguirão programar seus aplicativos para carregar previamente os *JWK Sets* de determinado PSP, de forma a agilizar o

[20] O padrão de certificados X.509 é definido pela *RFC* 5280, disponível em https://tools.ietf.org/html/rfc5280). Nele, o processo de validação da cadeia de certificação é descrito em detalhes.
[21] A definição do recurso denominado *Well-Known URIs* é feita pela RFC 8615, disponível em: https://tools.ietf.org/html/rfc8615.
[22] O formato do documento *host-meta* é definido pela RFC 6415, disponível em: https://tools.ietf.org/html/rfc6415.

processamento de transações via *QR Codes* dinâmicos quando o recebedor for aquele PSP.

Por fim, para garantir o não-repúdio das transações efetuadas por meio de *QR Codes* dinâmicos, recomenda-se que os participantes mantenham registros históricos das transações efetuadas, incluindo as respectivas estruturas *JWS*, certificados e chaves públicas relacionados a cada transação.

5. Certificados digitais

Esta seção apresenta os detalhes a respeito dos tipos de certificados a serem utilizados e descreve o processo de ativação, desativação e de verificação da revogação de certificados.

5.1. Certificados digitais a serem utilizados

Certificados para assinatura digital e autenticação e criptografia da conexão:

Tanto para autenticação e criptografia da conexão com as *APIs* do Pix como para assinatura digital das mensagens, todos os participantes devem utilizar certificados digitais ICP-Brasil no padrão SPB. As especificações para a geração e requisitos desse tipo de certificado constam no Manual de Segurança do SFN[23]. O Banco Central também utiliza certificados digitais padrão SPB para assinatura digital. Porém, apenas no caso do BC, para autenticação e criptografia da conexão são utilizados certificados SSL da cadeia v10 da ICP-Brasil.

Certificados *SSL* para sites/domínios de *QR Codes* dinâmicos:

Nos sites que hospedam *URLs* de *QR Codes* dinâmicos gerados pelo recebedor, não é necessário que o certificado associado seja padrão SPB, porém ele deve atender aos requisitos abaixo:

- Ser emitido por AC amplamente conhecida pelos diferentes navegadores e clientes de mercado;
- Ser do tipo *EV* ("*Extended Validation*" – Validação Estendida);
- Conter o(s) site(s)/domínios associado(s) aos *QR Codes* dinâmicos no campo *CN* (*"Common Name"*) ou *SAN* (*"Subject Alternative Name"*), considerando as restrições abaixo:
    - Para certificados de sites de *QR Codes* de homologação, o nome do servidor ("*host*") do site deverá, obrigatoriamente, terminar com "*-h*" (exemplo: "*qrcode-h.bancoxyz.com.br*"), conforme explicado na seção 4.1. No caso dos sites de *QR Codes* de produção, a única restrição é que o nome do *host* não deve terminar com "*-h*".
    - Os certificados poderão ser multidomínio, desde que, para certificados de sites de produção, nenhum dos *hosts* termine com "*-h*" e, para certificados de sites de homologação, todos os *hosts* terminem com "*-h*".
    - Não serão aceitos sites com *wildcard* (ex: "**.bancoxyz.com.br*") no certificado.

[23] Manual de Segurança do SFN, disponível para download na página https://www.bcb.gov.br/estabilidadefinanceira/comunicacaodados.

- Possuir o valor "Autenticação do Servidor" ("*Server Authentication*") no campo "Uso Avançado da Chave" ("*Extended Key Usage*");
- Ser cadastrado no Pix conforme especificado na seção 5.2.

Certificados para assinatura do *payload JWS* (*QR Codes* dinâmicos):

Assim como no caso anterior, o certificado vinculado à assinatura do *payload JWS* associado aos *QR Codes* dinâmicos não precisa ser padrão SPB, mas os requisitos abaixo devem ser atendidos:

- Ser emitido por AC amplamente conhecida pelos diferentes navegadores e clientes de mercado;
- Possuir o valor "Assinatura Digital" ("*Digital Signature*") no campo "Uso da Chave" ("*Key Usage*").

Conforme descrito na seção 4.2, este certificado, bem como sua cadeia completa de certificação (incluindo o certificado da AC raiz), constará no parâmetro *x5c* da estrutura *JWK*, que deve ser hospedada no mesmo site relacionado a *QR Codes* dinâmicos do PSP, portanto não é necessário ativá-lo no Pix.

5.2. Ativação de certificados digitais dos participantes

Para ativar um novo certificado digital, os participantes devem enviá-lo por meio do Sistema de Transferência de Arquivos (STA)[24], seguindo os códigos/nomes de arquivo abaixo:

Finalidade do certificado	Código do arquivo	Nome do arquivo
Autenticação da conexão	*CPIC*	*CERTPIC – Certificado Digital do participante no SPI para conexão*
Assinatura digital de mensagens	*CPIA*	*CERTPIA – Certificado Digital do participante no SPI para assinatura*
Certificado digital para sites de *QR Codes* dinâmicos	*CQRC*	*CERTQRC – Certificado Digital para sites de QR Codes Dinâmicos*

Tabela 5: Arquivos de certificado digital a serem enviados por meio do STA.

Regras para o envio de certificados:

- Os certificados devem ser enviados no formato *PEM* (codificação em *Base64*).
- Os certificados devem ser enviados sem incluir a cadeia de certificação ("*certificate chain*").
- Os arquivos de certificados enviados **não** devem incluir a chave privada

[24] Sistema de Transferência de Arquivos do Banco Central, disponível em: https://www.bcb.gov.br/acessoinformacao/sistematransferenciaarquivos

- Para envio de certificado digital do ambiente de Homologação, deverá ser utilizado o STA de homologação[25]. Para envio de certificado do ambiente de Produção, deverá ser usado o STA de produção[26].
- Ao receber um certificado via STA, o BC terá o prazo de 7 dias para ativá-lo no Pix. Portanto, recomenda-se que os participantes enviem novos certificados com antecedência igual ou superior a esse prazo.
- O envio do arquivo *CERTQRC* é permitido apenas para usuários com acesso ao serviço "*Sisbacen SCERTQRC*", que só deve ser concedido às pessoas devidamente autorizadas pelo PSP para essa função.
- Recomenda-se o envio dos arquivos de certificados em dias úteis, em horário comercial. Somente haverá suporte do BC para resolução de eventuais problemas no envio de arquivos durante o horário comercial.

Após o recebimento do certificado de assinatura digital ou de autenticação/criptografia da conexão, o BC efetua sua validação conforme requisitos definidos na seção 5.1. Caso a validação seja bem-sucedida, o STA informará, no campo "Estado", a mensagem "Arquivo aceito" e, no campo "Descrição complementar", a mensagem "Certificado digital aceito e ativado". Feito isso, o certificado será armazenado na base de dados do BC e estará pronto para utilização no Pix.

Para o caso específico dos certificados de sites de *QR Codes* dinâmicos, a verificação dos requisitos, incluindo a validação da cadeia de certificação completa, é de responsabilidade dos participantes. Após o recebimento desse tipo de certificado, o STA informará, no campo "Estado", a mensagem "Arquivo aceito" e, no campo "Descrição complementar", a mensagem "Certificado digital recebido".

Será disponibilizado pelo BC um arquivo contendo todos os certificados de sites de *QR Codes* dinâmicos cadastrados, conforme regras abaixo:

- O arquivo poderá ser obtido por meio de consulta à interface ARQ[27], nos caminhos abaixo:
  /api/v1/download/pub/cert/certqrc.zip (produção)
  /api/v1/download/pub/cert/certqrc-h.zip (homologação).
- Cada participante deverá realizar o download do arquivo no máximo uma vez a cada 24 horas.
- O participante deve manter cache do arquivo nas 24 horas seguintes a cada consulta.

[25] Disponível em https://sta-h.bcb.gov.br/sta.
[26] Disponível em https://sta.bcb.gov.br/sta.
[27] Mais informações sobre a interface ARQ estão disponíveis no Manual das Interfaces de Comunicação, cuja última versão disponível consta na página: https://www.bcb.gov.br/estabilidadefinanceira/comunicacaodados.

- Cada participante poderá consultar se o arquivo foi modificado e, caso não tenha havido alteração no arquivo desde o último download, não será necessário baixá-lo novamente.
- A interface ARQ de cada ambiente (Homologação ou Produção) disponibilizará no arquivo apenas os certificados de sites de *QR Codes* dinâmicos para aquele ambiente.
- É responsabilidade do participante pagador verificar o status de revogação do certificado do site associado ao *QR Code* do PSP recebedor. O arquivo de certificados disponibilizado pela interface ARQ terá atualização frequente, porém podem ocorrer revogações entre tais atualizações.
- Os participantes devem distribuir os novos certificados que forem ativados pelo BC para os seus softwares clientes em até 7 dias após a ativação.

Com base nas informações dos certificados que constarem no arquivo – incluindo o campo *CN* ou *SAN*, onde constará o site de *QR Code* dos demais participantes –, cada participante terá meios de implementar em seus aplicativos a validação, tanto do site como do certificado associado, no momento da leitura de um *QR Code* dinâmico, conforme descrito na seção 4.3 deste documento.

Cada PSP deve considerar que pode levar certo tempo para que os demais participantes propaguem nos seus aplicativos as informações dos certificados de sites de *QR Codes* dinâmicos recém cadastrados. Portanto, para evitar indisponibilidades devido a falhas de validação por parte dos aplicativos dos demais participantes, recomenda-se que cada PSP só implemente um novo certificado em seu(s) site(s) de *QR Codes* dinâmicos 7 dias após seu cadastro junto ao BC.

5.3. Boas práticas

As instituições participantes devem possuir processos adequados de gestão dos certificados digitais utilizados no âmbito do Pix. Os processos de gestão são obrigatórios e englobam a geração, a guarda, a ativação e a revogação desses certificados digitais. Nesse contexto, é imprescindível zelar pela guarda e integridade das chaves criptográficas privadas, utilizando mecanismos de segurança que garantam o seu acesso somente a pessoas autorizadas pelo participante. Recomenda-se a utilização de dispositivos de criptografia baseados em hardware (HSMs) para armazenamento das chaves privadas dos certificados.

Recomenda-se ainda que cada instituição utilize certificados distintos, exclusivos para cada finalidade.

No intuito de evitar eventuais indisponibilidades devido à troca de certificados, poderão estar ativos simultaneamente múltiplos certificados por participante, inclusive para a mesma finalidade. O mesmo se aplica aos certificados do BC. Nesse sentido, um mesmo PSP também poderá ter mais de um site/certificado de *QR Codes* dinâmicos.

5.4. Ativação de certificados digitais do BC

5.4.1. Comunicação prévia

A ativação de novos certificados do BC será comunicada com antecedência de, no mínimo, 7 dias, por meio de Comunicado Sisbacen. Os novos certificados serão publicados no portal da RSFN[28], juntamente com os demais certificados ativos.

5.4.2. Certificados de assinatura digital

Para assinatura digital, o BC utiliza certificados digitais ICP-Brasil no padrão SPB.

Processo de ativação:

Passado o prazo definido no comunicado descrito no item 5.4.1, o BC começará a assinar mensagens com o novo certificado. A critério do BC, a transição entre o certificado anterior e o novo poderá ser escalonada, de forma que inicialmente apenas um percentual das mensagens sejam assinadas com o novo certificado.

5.4.3. Certificados de autenticação e criptografia da conexão:

O BC utiliza certificados SSL da cadeia v10 da ICP-Brasil para autenticação e criptografia da conexão.

Processo de ativação:

Passado o prazo definido no comunicado descrito no item 5.4.1, o BC ativará o novo certificado nos seus sites. A critério do BC, a ativação do novo certificado poderá ser gradual, em um site por vez. Cada participante deve estar preparado para aceitar mais de um certificado ativo pelo BC e deve efetuar, no mínimo, as validações abaixo:

- O certificado deve ser emitido por AC vinculada à cadeia v10 da ICP-Brasil[29];
- *URL* do Pix ("**.pi.rsfn.net.br*") deve constar no *CN* do certificado;
- O certificado não pode estar expirado.

5.5. Desativação de certificados digitais

[28] Disponível somente para os participantes da RSFN, no endereço: http://www.rsfn.net.br
[29] O certificado raiz da cadeia deve ser o da "Autoridade Certificadora Raiz Brasileira v10", disponível em http://acraiz.icpbrasil.gov.br/credenciadas/RAIZ/ICP-Brasilv10.crt.

Todos os certificados – tanto do BC como dos participantes – serão automaticamente desativados 24 horas antes de sua data de expiração. Tentativas de autenticação com certificados desativados, bem como as mensagens e requisições assinadas com chaves privadas associadas a certificados desativados serão rejeitadas pelo BC.

Caso um participante precise desativar determinado certificado, o seguinte processo deve ser seguido:

1. O participante deve enviar mensagem ao Banco Central por meio do BC Correio[30] para a caixa DEINF/Pix.
2. A mensagem deve ser emitida por um dos contatos cadastrados no sistema de cadastro e monitoramento do Pix no BC, a saber: Diretor Pix, Diretor SPI ou Responsável Técnico do DICT. O BC poderá entrar em contato por e-mail ou telefone para verificar a identidade do emissor.
3. A mensagem deve incluir as seguintes informações:
    a. Assunto: "Pix - Desativação de certificado";
    b. Dados do certificado a ser desativado: autoridade certificadora emissora e número de série;
    c. Justificativa técnica para a desativação.
4. O participante deve entrar em contato com a Central de Atendimento do Pix[31] para solicitar a desativação, citando o número do BC Correio enviado e indicando a urgência da desativação, que deverá ser "Prioritária" (atendimento na Central de Atendimento, 24x7) ou "Não Prioritária" (atendimento na Central de Atendimento, somente em dias úteis, entre 9h e 18h). Deve haver justificativa quando a urgência indicada for "Prioritária". Para desativações de certificados em ambiente de homologação, todas as solicitações serão sempre "Não Prioritárias".

    Observação: o BC Correio não é um sistema 24x7 e pode estar sujeito a manutenções e indisponibilidade fora do horário comercial.

Caso o BC precise desativar um de seus certificados, será enviado Comunicado Sisbacen aos participantes informando o certificado a ser desativado e a data em que ele não deverá mais ser aceito pelos participantes do ecossistema.

5.6. Verificação da revogação de certificados

Tanto o BC como os demais participantes do Pix deverão verificar que nenhum certificado utilizado no ecossistema foi revogado. Porém, considera-se tecnicamente

[30] A aplicação BC Correio está disponível em: https://bccorreio.bcb.gov.br/bccorreio/.
[31] A Central de Atendimento do Pix está disponível nos telefones (61) 3414-5100 e (61) 3553-5100 ou no e-mail suporte.pix@bcb.gov.br.

inviável efetuar essa verificação de forma *online* – a cada conexão ou mensagem – por dois motivos principais:

- No Pix, os sistemas dos participantes, PSTIs e BC estão conectados apenas à RSFN e, portanto, não possuem conectividade com a Internet. Por esse motivo, tais sistemas não deverão conseguir acessar os pontos de distribuição de *LCRs*[32], sites *OCSP*[33], etc.
- A consulta de forma *online*, a cada conexão ou mensagem, poderia impactar o tempo total de processamento das transações, resultando em uma experiência ruim para os usuários finais.

Dado o exposto acima, o Banco Central efetuará a verificação da revogação de certificados por meio de processo separado e assíncrono, porém frequente. Caso o certificado de algum participante conste como revogado, o BC enviará notificação para a instituição via BC Correio e deixará de aceitar transações de/para essa instituição. É recomendado que todos os participantes do ecossistema implementem a verificação da revogação de certificados de forma similar à realizada pelo BC. Caso algum certificado do BC conste como revogado, o participante deverá rejeitar a conexão ou mensagem, e enviar notificação ao Departamento de Tecnologia da Informação (DEINF) do Banco Central por meio do BC Correio.

Caso o status de revogação de determinado certificado do BC não possa ser verificado devido a eventual indisponibilidade ou erro inesperado, o participante deverá notificar o DEINF, porém as conexões ou mensagens do BC deverão continuar sendo aceitas temporariamente, enquanto a resolução da situação não for informada pelo BC. Assim, evita-se indisponibilidades do Pix devido a problemas externos – por exemplo, nas próprias ACs.

Além de verificar o status de revogação dos certificados do BC, os participantes devem verificar também a eventual revogação dos certificados vinculados aos sites de *QR Code* e à assinatura do *JWS* dos demais participantes do ecossistema. A transação de *QR Code* deve ser rejeitada caso algum dos certificados esteja revogado ou caso não seja possível verificar sua revogação.

[32] *LCRs*: Listas de Certificados Revogados providas pelas Autoridades Certificadoras.
[33] *OCSP: Online Certificate Status Protocol,* definido pela RFC 6960, disponível em https://tools.ietf.org/html/rfc6960.

6. Implementação segura de aplicativos, *APIs* e outros sistemas

Os aplicativos, *APIs*[34] e outros sistemas relacionados ao Pix devem ser desenvolvidos seguindo os princípios de proteção de dados pessoais previstos no artigo 6º e outros dispositivos da Lei Geral de Proteção de Dados (LGPD)[35]. De todo modo, é imprescindível que todos os sistemas envolvidos no Pix sejam desenvolvidos e implementados de forma segura. Os itens abaixo tratam dos aspectos de segurança obrigatórios na implementação desses sistemas.

1. Eventuais *APIs* ou outros sistemas acessados por aplicativos do participante devem implementar criptografia na comunicação, além de mecanismos de autenticação forte do *software* cliente, por exemplo, por meio de *mTLS*[36], de forma a:
    a. garantir que os *softwares* clientes das *APIs* ou sistemas sejam apenas os aplicativos da instituição, impedindo o acesso de robôs e *scripts* automatizados;
    b. impedir ataques de *man-in-the-middle*[37].
2. De forma similar ao item anterior, os aplicativos e outros *softwares* clientes dos participantes devem adotar técnicas, como o *mTLS* já citado, para garantir que sua comunicação seja cifrada e ocorra apenas com as *APIs* e sistemas desejados, não permitindo ataques de *man-in-the-middle* ou qualquer manipulação de sua comunicação.
3. Os aplicativos e outros *softwares* clientes dos participantes devem possuir mecanismos de segurança para impedir sua engenharia reversa, descompilação, manipulação de código, modificação de credenciais ou parâmetros de segurança, dentre outras técnicas que resultem na sua adulteração ou comprometimento.
4. A segurança das *APIs* e outros sistemas relacionados ao Pix deve estar implementada majoritariamente na parte servidora, não contando apenas

[34] O termo *API* utilizado nesta seção refere-se a quaisquer *APIs* utilizadas pelos participantes ao longo de toda a cadeia de provimento de funcionalidades do Pix para seus clientes. Vale ressaltar que a *API Pix*, detalhada no Manual de Padrões para Iniciação do Pix, possui requisitos de segurança próprios que constam naquele Manual.

[35] Lei Geral de Proteção de Dados (LGPD): http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

[36] *mTLS* ou *Mutual TLS authentication*: técnica de autenticação mútua utilizando o protocolo *TLS*, em que o servidor se identifica com o seu certificado e requer que o cliente se autentique com um certificado próprio.

[37] *man-in-the-middle*: ataque por meio do qual o atacante intercepta e modifica a comunicação entre o cliente e o servidor, podendo se passar como uma das partes envolvidas. Mais detalhes disponíveis em https://csrc.nist.gov/glossary/term/man_in_the_middle_attack.

com a segurança do *software* cliente ou aplicativo. Evita-se, assim, que um agente malicioso explore eventual falha do cliente ou aplicativo e obtenha acesso indevido.

5. Os sistemas e *APIs* devem fornecer apenas as informações estritamente necessárias para o correto funcionamento dos aplicativos do participante.
    a. No caso de consultas por chaves Pix e transações utilizando *QR Code*, informações como CPF completo (sem máscara), dados de agência e conta de destinatários de pagamentos via Pix, bem como informações para fins de segurança vinculadas às chaves Pix devem ser de uso exclusivo dos sistemas internos do participante e, portanto, não devem ser expostas aos seus aplicativos e *softwares* clientes.
    b. A restrição acima não se aplica apenas no caso de transações Pix por meio de inserção manual de dados bancários nos ambientes Pix e *Open Finance*, onde os dados de agência e conta precisarão ser exibidos.
6. Conforme disposto no Regulamento do Pix[38], a base interna de chaves Pix de cada PSP deve ter mecanismos para:
    a. prevenir ataques de leitura de chaves, de forma equivalente aos mecanismos que constam no item 13 do Manual Operacional do DICT[39];
    b. limitar o número de requisições oriundas de um mesmo *software* cliente ou aplicativo, de forma equivalente ao controle disposto no item 15 do Manual Operacional do DICT.
7. A realização de consultas de chaves e transações Pix por meio do site *web* do participante só deve ser permitida a usuários devidamente logados, e deve estar sujeita a mecanismos de segurança que impeçam o uso de robôs e a automatização de consultas e transações. Dentre os mecanismos possíveis, constam: autenticação do usuário por dois fatores, *CAPTCHA*, *token* em dispositivo cadastrado previamente, etc.

[38] Resolução BCB nº 1, que institui o arranjo de pagamentos Pix e aprova seu Regulamento: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=1

[39] Manual Operacional do DICT: https://www.bcb.gov.br/estabilidadefinanceira/pix

7. Logs de auditoria

Esta seção trata dos logs de auditoria que devem ser mantidos por todos os participantes do Pix, com o objetivo de permitir a rastreabilidade e auditoria das mensagens transmitidas e recebidas, bem como das transações realizadas no âmbito do ecossistema de pagamentos instantâneos.

7.1. Requisitos gerais

- A data e horário de cada entrada no log deverá ser registrada no fuso horário *UTC*.
- Recomenda-se que os registros de log sejam armazenados de forma criptografada e com acesso devidamente controlado e autenticado.
- O prazo de retenção dos logs é de 10 (dez) anos, contados a partir da data de geração de cada registro.
- Caso o Banco Central solicite os logs, a instituição deverá fornecê-los descriptografados, no formato requerido pelo BC.
- Todos os certificados utilizados no âmbito do Pix, incluindo os já desativados, deverão ser armazenados por cada participante para eventual consulta histórica de mensagens – e respectiva validação da assinatura digital, caso seja necessário.

7.2. Logs da ICOM/SPI

Na comunicação do PSP com a ICOM/SPI, todo o conteúdo *XML* (*tag* <*envelope*>) das mensagens enviadas e recebidas pelo PSP deve ser armazenado em log. Sendo assim, o log deve conter não apenas a mensagem propriamente dita, mas também as informações de assinatura digital, incluindo dados do certificado digital e dos algoritmos utilizados, além de outras *tags* e cabeçalhos relacionados à mensagem.

É recomendado que o PSP armazene os cabeçalhos *HTTP* das requisições e respectivas respostas da ICOM/SPI. Caso não sejam armazenados os cabeçalhos *HTTP* completos, é obrigatório que pelo menos o cabeçalho "*PI-ResourceId*", quando existente, seja armazenado.

7.3. Logs do DICT

Toda comunicação do participante com o DICT deverá ser registrada em log, independentemente da operação realizada, seja ela uma consulta ou atualização de uma entrada no diretório, uma criação de reivindicação ou disputa, uma reconciliação, etc. Todo o conteúdo *XML* das requisições e respostas deverão ser registrados no log, incluindo cabeçalhos, dados de assinatura digital, etc.

Assim como no caso da ICOM, é recomendado que o participante armazene os cabeçalhos *HTTP* das requisições e respectivas respostas do DICT. Caso não sejam armazenados os cabeçalhos *HTTP* completos, é obrigatório que pelo menos os cabeçalhos abaixo, quando existentes, sejam armazenados:

- *PI-RequestingParticipant*;
- *PI-PayerId*;
- *PI-EndToEndId*.